are allowed access to each cartridge, and only certain users are allowed to define who has access to that data.

While the preferred embodiments of the present invention have been illustrated in detail, it should be apparent that modifications and adaptations to those embodiments may occur to one skilled in the art without departing from the scope of the present invention as set forth in the following claims.

I claim:

SUB A47

1. A portable security system for managing access to a portable data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, said portable security system comprising:

a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive; and

a computer processor mounted in said portable data storage cartridge and coupled to said wireless interface; said computer processor powered by said wireless interface and receiving and transmitting data to said data storage drive via said wireless interface; said computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user

activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface.

2. The portable security system of Claim 1, wherein said wireless interface comprises an RF interface.

3. The portable security system of Claim 1, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer processor conducts said combination by decrypting said user authentication message by said user decrypting key.

4. The portable security system of Claim 3, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic algorithm.

5. The portable security system of Claim 4, wherein said user authentication message is encrypted by a sender private key and a receiver public key, and wherein said public key cryptographic algorithm decrypts said user authentication message employing a

receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

6. The portable security system of Claim **1**, wherein said computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table.

7. The portable security system of Claim **1**, wherein said computer processor user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct.

8. The portable security system of Claim **1**, wherein said computer processor user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct.

9. The portable security system of Claim 1, wherein said computer processor additionally comprises a nonvolatile memory storing said user table.

10. The portable security system of Claim 1, wherein said computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user; and wherein said computer processor additionally, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user, and transmitting said class authorization or denial to said data storage drive via said wireless interface.

11. The portable security system of Claim 10, wherein said computer processor user table additionally comprises any class membership of each said user, wherein said user may be authorized

with respect to said class table either by said class authorization or by said user authorization.

12. The portable security system of Claim **10**, wherein said computer processor user table and said class table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table.

13. The portable security system of Claim **10**, wherein said computer processor additionally comprises a nonvolatile memory storing said user table and said class table.

14. The portable security system of Claim **1**, wherein said data stored in said data storage media is encrypted, wherein said computer processor user table permitted activities comprise at least 1) read access to data stored in said data storage media, and wherein said user authorization for said read access additionally comprises a decryption key for said encrypted stored data.

15. A data storage cartridge for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, comprising:

data storage media mounted in said data storage cartridge for storing said data for said read/write access;

a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive; and

a computer processor mounted in said portable data storage cartridge and coupled to said wireless interface; said computer processor powered by said wireless interface and receiving and transmitting data to said data storage drive via said wireless interface; said computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user

activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface.

16. The data storage cartridge of Claim **15**, wherein said wireless interface comprises an RF interface.

17. The data storage cartridge of Claim **15**, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer processor conducts said combination by decrypting said user authentication message by said user decrypting key.

18. The data storage cartridge of Claim **17**, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic algorithm.

19. The data storage cartridge of Claim **18**, wherein said user authentication message is encrypted by a sender private key and a receiver public key, and wherein said public key cryptographic algorithm decrypts said user authentication message employing a

receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

20. The data storage cartridge of Claim **15**, wherein said computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table.

21. The data storage cartridge of Claim **15**, wherein said computer processor user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct.

22. The data storage cartridge of Claim **15** wherein said computer processor user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct.

23. The data storage cartridge of Claim **15**, wherein said computer processor additionally comprises a nonvolatile memory storing said user table.

24. The data storage cartridge of Claim **15**, wherein said computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user; and wherein said computer processor additionally, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user, and transmitting said class authorization or denial to said data storage drive via said wireless interface.

25. The data storage cartridge of Claim **24**, wherein said computer processor user table additionally comprises any class membership of each said user, wherein said user may be authorized

with respect to said class table either by said class authorization or by said user authorization.

26. The data storage cartridge of Claim **24**, wherein said computer processor user table and said class table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table.

27. The data storage cartridge of Claim **24**, wherein said computer processor additionally comprises a nonvolatile memory storing said user table and said class table.

28. The data storage cartridge of Claim **15**, wherein said data stored in said data storage media is encrypted, wherein said computer processor user table permitted activities comprise at least 1) read access to data stored in said data storage media, and wherein said user authorization for said read access additionally comprises a decryption key for said encrypted stored data.

29. A method for providing a portable secure interface to a data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, and a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive, said data storage cartridge having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user, said method comprising the steps of:

receiving said user authentication messages from said data storage drive via said wireless interface;

combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity; and

transmitting said user authorization or denial to said data storage drive via said wireless interface.

30. The method of Claim **29**, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said combining step comprises decrypting said user authentication message by said user decrypting key.

31. The method of Claim **30**, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic algorithm.

32. The method of Claim **31**, wherein said user authentication message is encrypted by a sender private key and a receiver public key, wherein said public key cryptographic algorithm decrypts said user authentication message employing a receiver private key and said sender public key, and wherein said combining step comprises decrypting said user authentication message by said receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

33. The method of Claim **29**, wherein said user table comprises a plurality of said permitted activities, selected ones of which

each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table; and wherein said transmitting step comprises transmitting authorization to conduct the selected said user permitted activities said user is authorized to conduct.

34. The method of Claim **29**, wherein said user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct; and wherein said transmitting step additionally comprises identifying said user permitted activities from said separate entries.

35. The method of Claim **29**, wherein said step of providing said user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct; and wherein said transmitting step additionally comprises identifying said user permitted activities from said user separate entry.

36. The method of Claim **29**, wherein said data storage cartridge additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user;

wherein said combining step additionally comprises, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user; and

wherein said transmitting step additionally comprises transmitting said class authorization or denial to said data storage drive via said wireless interface.

37. The method of Claim **36**, wherein said user table additionally comprises any class membership of each said user; and wherein said combining step additionally authorizes said user with respect to said class table either by said class authorization or by said user authorization.

38. The method of Claim **36**, wherein said user table and said class table comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table; and wherein said transmitting step comprises transmitting authorization to conduct the selected said user and said class permitted activities said user is authorized to conduct.

39. The method of Claim **29**, wherein said data stored in said data storage media is encrypted, wherein said step of providing said user table permitted activities comprises providing at least 1) read access to data stored in said data storage media, and wherein said step of transmitting said user authorization for said read access additionally comprises transmitting a decryption key for said encrypted stored data.

40. A computer program product usable with a programmable computer processor having computer readable program code embodied therein for providing a secure interface to a data storage cartridge, said programmable computer processor mounted in said data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, and a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive, said computer program product comprising:

computer readable program code which causes said programmable computer processor to provide a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user;

computer readable program code which causes said programmable computer processor to receive said user authentication messages from said data storage drive via said wireless interface;

computer readable program code which causes said programmable computer processor to combine said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity; and

computer readable program code which causes said programmable computer processor to transmit said user authorization or denial to said data storage drive via said wireless interface.

41. The computer program product of Claim **40**, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer readable program code additionally causes said programmable computer processor to conduct said combination by decrypting said user authentication message by said user decrypting key.

42. The computer program product of Claim **41**, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic algorithm.

43. The computer program product of Claim 42, wherein said user authentication message is encrypted by a sender private key and a receiver public key, wherein said public key cryptographic algorithm decrypts said user authentication message employing a receiver private key and said sender public key, and wherein said computer readable program code additionally causes said programmable computer processor, in conducting said combination, to decrypt said user authentication message by said receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

44. The computer program product of Claim 40, wherein said computer readable program code additionally causes said programmable computer processor to provide in said user table a plurality of said permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table.

45. The computer program product of Claim 40, wherein said computer readable program code additionally causes said

programmable computer processor to provide in said user table a separate entry for each said user identifier and said permitted activity said user is authorized to conduct.

46. The computer program product of Claim 40, wherein said computer readable program code additionally causes said programmable computer processor to provide in said user table a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct.

47. The computer program product of Claim 40, wherein said computer readable program code additionally causes said programmable computer processor:

to provide a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user;

in conducting said combination, upon receiving said user authentication messages from said data storage drive via said wireless interface, to combine said user authentication message

with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user; and

in conducting said transmission, to transmit said class authorization or denial to said data storage drive via said wireless interface.

48. The computer program product of Claim **47**, wherein said computer readable program code additionally causes said programmable computer processor to provide in said user table any class membership of each said user, wherein said user may be authorized with respect to said class table either by said class authorization or by said user authorization.

49. The computer program product of Claim **47**, wherein said computer readable program code additionally causes said programmable computer processor to provide in said user table and said class table a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table.

50. The computer program product of Claim **40**, wherein said data stored in said data storage media is encrypted, and wherein said computer readable program code additionally causes said programmable computer processor to provide in said user table permitted activities comprising at least 1) read access to data stored in said data storage media, and wherein said computer readable program code additionally causes said programmable computer processor to transmit in said user authorization for said read access, a decryption key for said encrypted stored data.